Distribuire DNS VNF con rete SRIOV su Openstack CVIM - Esempio di configurazione per Prime Network Registrar (DNS)

Sommario

Introduzione

In questo documento viene descritta l'implementazione dettagliata del protocollo CPNR su OpenStack Cisco Virtualized Infrastructure Manager (CVIM) utilizzando SR-IOV e il collegamento di Active-Backup.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Familiarità con i concetti di OpenStack e Single Root Input/Output Virtualization (SR-IOV)
- Conoscenza operativa dei comandi e delle reti di Cisco Virtual Interface Manager (VIM), Cisco Elastic Services Controller e Linux

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi

Premesse

Nell'attuale scenario di rete, le funzioni di rete virtuali (VNF) svolgono un ruolo critico nel consentire servizi di rete agili, scalabili ed efficienti. Per le VNF che richiedono una connettività di rete ad alte prestazioni, SR-IOV è una tecnologia comunemente utilizzata. SR-IOV consente alle VNF di ignorare lo switch virtuale dell'hypervisor e di accedere direttamente alle risorse fisiche del controller di interfaccia di rete (NIC), riducendo in tal modo la latenza e aumentando il throughput.

Configurazione

Prima di procedere con la distribuzione, verificare che i prerequisiti siano soddisfatti.

1. Requisiti hardware

- Schede di rete compatibili con SR-IOV:
  - Almeno due schede di interfaccia di rete fisiche compatibili con SR-IOV con SR-IOV abilitato nell'interfaccia UEFI (Unified Extensible Firmware Interface) del BIOS.
  - Esempio:sriov0mappato al nodo NUMA (Non-Uniform Memory Access) 0 e sriov1mappato al nodo NUMA 1.

- Host compatibili con NUMA:
  - I nodi di elaborazione devono supportare l'architettura NUMA.
  - Il supporto NUMA deve essere abilitato nel BIOS/UEFI degli host.

2. Identificazione delle schede NIC Intel

Le schede NIC Intel XL710 e E810CQDA2 sono comunemente utilizzate per il networking SR-IOV

ad alte prestazioni. Per verificare il modello della scheda NIC sull'host, attenersi alla seguente procedura:

Passaggio 1. Uso del comando lspci

Eseguire questo comando per elencare le periferiche PCI (Peripheral Component Interconnect) correlate ai controller di rete:

```
lspci | grep -i ethernet
```

Esempio:

```
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ (rev 02)
82:00.0 Ethernet controller: Intel Corporation Ethernet Controller E810-C for QSFP (rev 03)
```

Passaggio 2. Verifica di XL710

Se la scheda NIC è Intel XL710, è possibile visualizzare il controller Ethernet XL710 nell'output.

Passaggio 3. Verifica di E810CQDA2

Se la scheda NIC è Intel E810CQDA2, è possibile visualizzare l'output del controller Ethernet E810-Cin.

Passaggio 4. Conferma del supporto del driver

Per controllare il driver della scheda NIC in uso, eseguire:

```
ethtool -i
```

Esempio di output per XL710:

```
driver: i40e
version: 2.13.10
```

Esempio di output per E810CQDA2:

```
driver: ice
version: 1.7.12
```

Verificare che la versione del driver corrisponda alla matrice di compatibilità per la distribuzione OpenStack e Linux.

3. Configurazione BIOS/UEFI

- Abilitare SR-IOV:

Verificare che SR-IOV sia abilitato nel BIOS/UEFI dei server.

- Tecnologia di virtualizzazione per I/O diretto (VT-d)/AMD-Vi:

Intel VT-d o AMD-Vi devono essere abilitati per le funzionalità PCI passthrough e SR-IOV.

4. Installazione di OpenStack

- Servizi principali OpenStack:

Accertarsi che i servizi OpenStack come Nova, Neutron, Glance e Keystone siano installati e configurati.

- Configurazione neutroni:

Neutron deve supportare sia Openvswitch (OVS) per le reti di orchestrazione/gestione che SR-IOV per le reti di applicazioni/servizi.

- Configurazione SR-IOV:

I nodi di elaborazione devono essere configurati in modo da supportare SR-IOV, con le funzioni virtuali (VF) create sulle schede di interfaccia di rete.

5. Immagine VNF Cisco Prime Network Registrar (CPNR)

- Compatibilità immagine VNF:

L'immagine VNF CPNR deve supportare le interfacce SR-IOV e includere i driver necessari.

- Carica in breve:

Assicurarsi che l'immagine VNF CPNR sia disponibile in OpenStack Glance.

6. Accesso amministrativo

- CLI di OpenStack:

Garantire l'accesso all'interfaccia CLI di OpenStack per la creazione di reti, versioni e l'avvio di VNF.

- Privilegi root o admin:

Accesso root o amministrativo per configurare la rete sull'host Linux e all'interno del VNF.

Panoramica dell'architettura

Diagramma connettività interfaccia di rete VNF

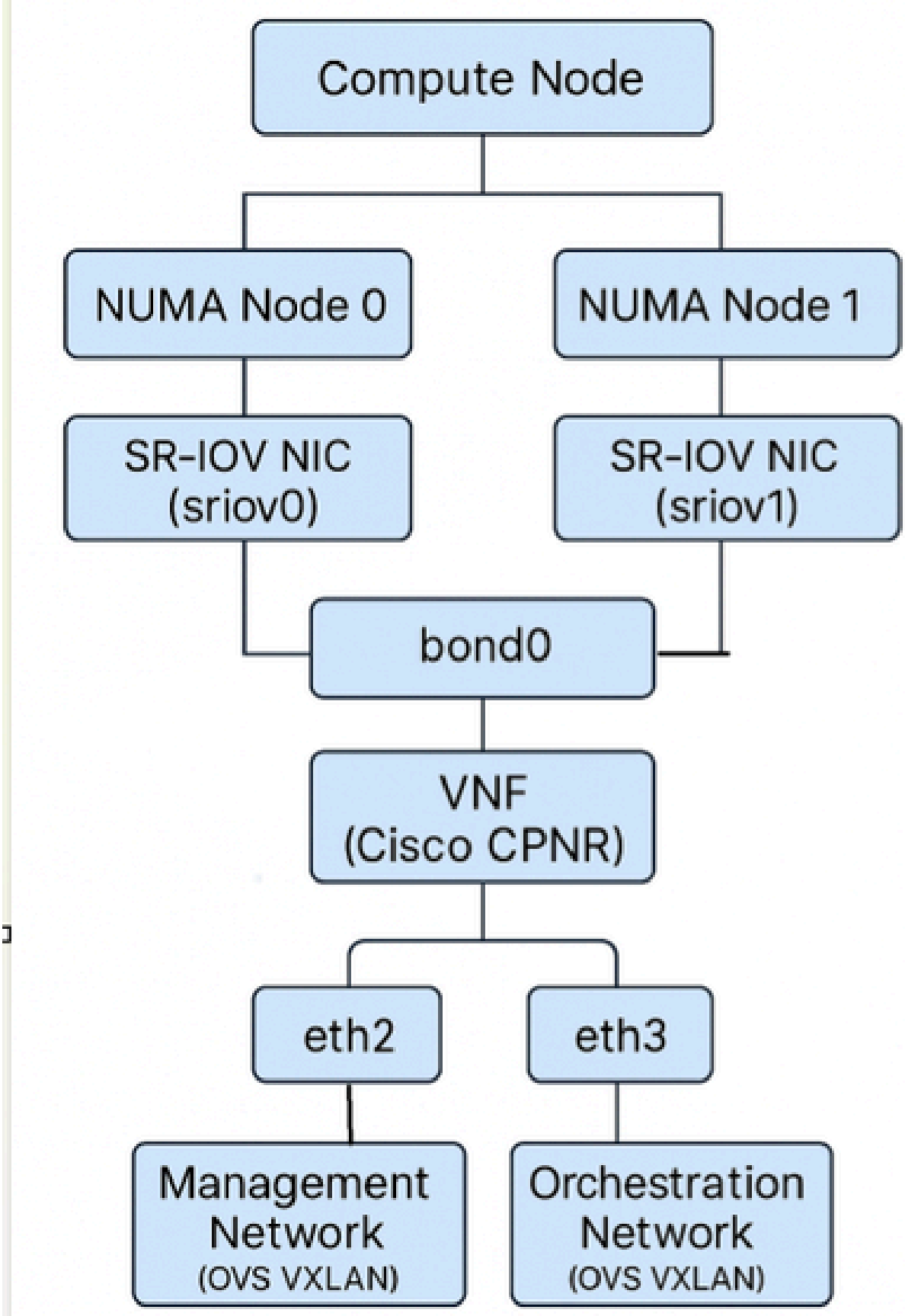
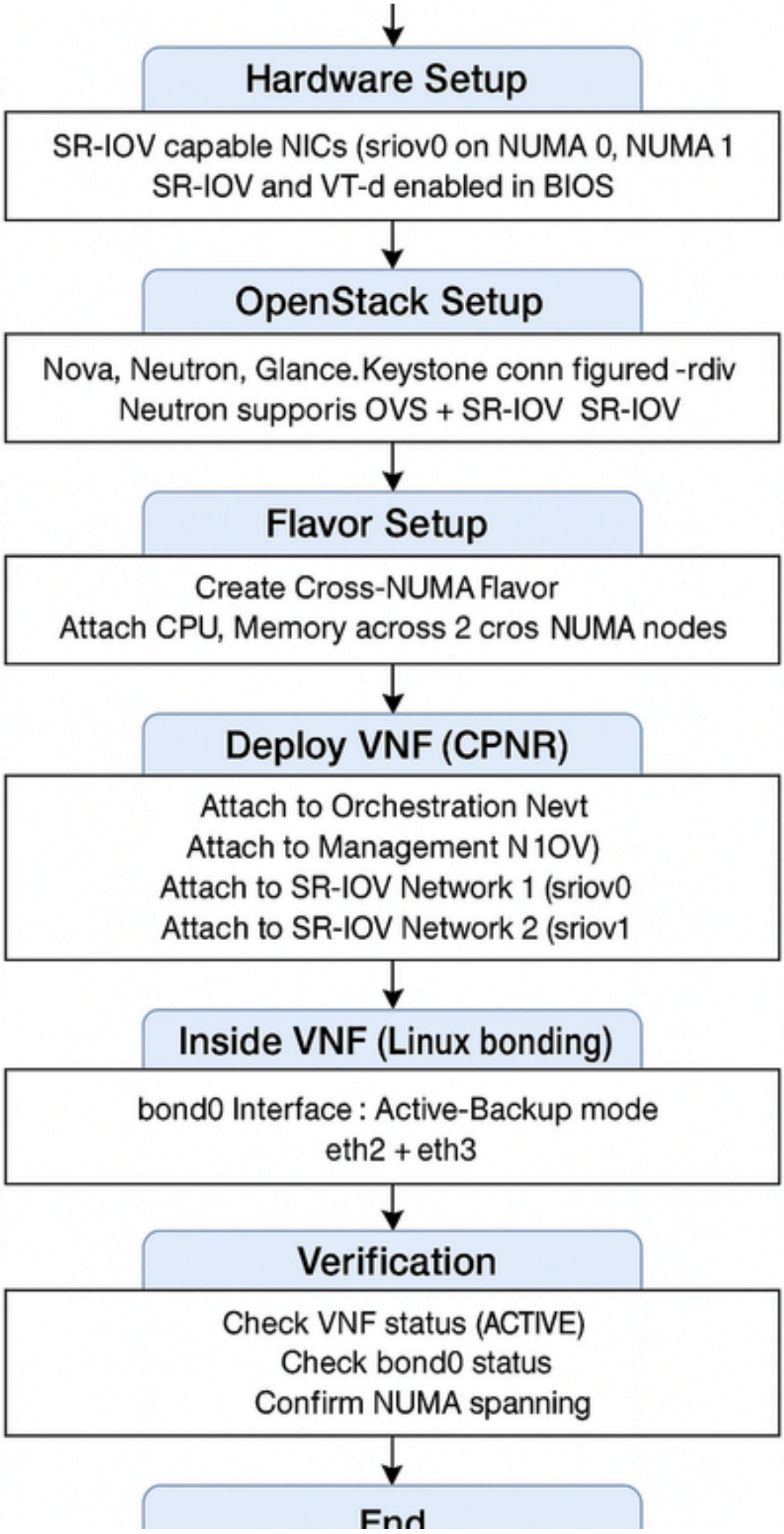


Diagramma di flusso


Hardware Setup
SR-IOV capable NICs (sriov0 on NUMA 0, NUMA 1
SR-IOV and VT-d enabled in BIOS
OpenStack Setup
Nova, Neutron, Glance.Keystone conn figured -rdiv
Neutron supporis OVS + SR-IOV SR-IOV
Flavor Setup
Create Cross-NUMA Flavor
Attach CPU, Memory across 2 cros NUMA nodes
Deploy VNF (CPNR)
Attach to Orchestration Nevt
Attach to Management N1OV)
Attach to SR-IOV Network 1 (sriov0
Attach to SR-IOV Network 2 (sriov1
Inside VNF (Linux bonding)
bond0 Interface : Active-Backup mode
eth2 + eth3
Verification
Check VNF status (ACTIVE)
Check bond0 status
Confirm NUMA spanning
End

2. Collegamento Active-Backup:

    - Viene creata un'interfaccia bond0 utilizzando le schede di interfaccia di rete SR-IOV (eth2 da sriov0 e eth3 da sriov1).
    - La modalità Active-Backup garantisce ridondanza e tolleranza di errore senza richiedere configurazioni di switch-side.

3. Reti OpenStack:

    - Reti di orchestrazione e gestione: Basato su openvswitch per il controllo e l'amministrazione del traffico.
    - Reti di applicazioni/servizi: Basato su SR-IOV per traffico ad alte prestazioni.

Perché è necessaria la modalità Cross-NUMA

1. Reti compatibili con NUMA in OpenStack

NUMA è un'architettura di memoria in cui ciascuna CPU (e la relativa memoria locale e i dispositivi) sono raggruppati in un nodo NUMA. In OpenStack, il posizionamento con riconoscimento NUMA assicura che le VNF siano assegnate in modo ottimale alle risorse sullo stesso nodo NUMA per ridurre al minimo la latenza e ottimizzare le prestazioni.

- Le schede di interfaccia di rete SR-IOV sono locali NUMA:
    - Ogni NIC fisica è legata a un nodo NUMA specifico. Ad esempio:
        - sriov0 è collegato al nodo NUMA 0.
        - sriov1 è collegato al nodo NUMA 1.
- Limitazione modalità NUMA singola:
    - Quando un VNF viene avviato in modalità NUMA singola, OpenStack consente solo al VNF di connettersi alle schede NIC locali al nodo NUMA su cui è avviato il VNF. Ciò significa che:
        - Se il VNF viene avviato su NUMA 0, può connettersi solo alle schede NIC su sriov0.
        - Se il VNF viene avviato sul NUMA 1, può connettersi solo alle schede NIC sul router sriov1.

2. Perché è necessaria la modalità Cross-NUMA

Il CPNR VNF richiede l'accesso a:

- Rete di orchestrazione (Openvswitch, agnostica NUMA)
- Rete di gestione (Openvswitch, indipendente da NUMA)
- Rete SR-IOV 1: Connesso a tosriov0(nodo NUMA 0)
- Rete SR-IOV 2: Connesso a tosriov1(nodo NUMA 1).

In questa implementazione, la VNF CPNR richiede l'accesso alle schede NIC SR-IOV sia da NUMA 0 (sriov0) che da NUMA 1 (sriov1) per fornire ridondanza ed elevata disponibilità. A tal fine:

- Il VNF deve essere avviato in modalità cross-NUMA, che consente a OpenStack di allocare CPU, memoria e NIC da più nodi NUMA.
- In questo modo il VNF può connettersi alle schede NIC su sriov0 e sriov1, consentendo l'utilizzo di entrambe le porte SR-IOV in una configurazione con collegamento Active-Backup.

Limitazione delle dimensioni della traccia per le porte OVS

Cos'è Conntrack?

Conntrack è una funzionalità del kernel Linux utilizzata per tenere traccia delle connessioni di rete, in particolare per le regole NAT (Network Address Translation) e firewall. Per le porte basate su OVS in OpenStack, la funzione conntrack viene utilizzata per gestire lo stato della connessione e applicare le regole dei gruppi di sicurezza.

Effetti di Conntrack sulle porte OVS

1. Tabella Conntrack:

    - Ogni connessione attiva utilizza una voce nella tabella di connessione.
    - La dimensione della tabella di connessione è limitata dal parametro thenf_conntrack_max.

2. Limite predefinito:

    - Per impostazione predefinita, la dimensione della tabella di traccia è di 65536 voci. Per i carichi di lavoro con alte velocità di connessione (ad esempio, le VNF con molti flussi simultanei), questo limite può essere rapidamente esaurito, con conseguenti pacchetti scartati.

3. Impatto sulle porte OVS:

    - Se la tabella di connessione è piena, le nuove connessioni vengono interrotte, con un conseguente impatto negativo sulle prestazioni VNF.
    - Ciò è particolarmente rilevante per le reti di orchestrazione e gestione, che utilizzano porte OVS.

Come mitigare i limiti della traccia di connessione

1. Aumenta dimensioni tabella di controllo:

    - Visualizzare il limite corrente:

```
sysctl net.netfilter.nf_conntrack_max
```

- Aumentare il limite:

```
sysctl -w net.netfilter.nf_conntrack_max=262144
```

- Rendere persistente la modifica:

```
echo "net.netfilter.nf_conntrack_max=262144" >> /etc/sysctl.conf
```

2. Monitoraggio utilizzo di Conntrack:

   Controllare le statistiche di traccia:

```
cat /proc/sys/net/netfilter/nf_conntrack_count
```

3. Ottimizza regole gruppo di sicurezza:

   Ridurre il numero di regole applicate alle porte OVS per ridurre al minimo il sovraccarico di traccia.

Risoluzione dei problemi Conntrack con SR-IOV

1. Eliminazione della dipendenza dalla traccia

Le porte SR-IOV ignorano il datapath OVS e le funzionalità del kernel Linux come conntrack. In questo modo si rimuove completamente il sovraccarico di verifica delle connessioni.

2. Maggiore scalabilità

A differenza delle porte OVS, che sono limitate dalle dimensioni della tabella di connessione (nf_conntrack_max), le porte SR-IOV possono gestire un numero virtualmente illimitato di connessioni.

3. Latenza ridotta

Scaricando l'elaborazione dei pacchetti sull'hardware NIC, le porte SR-IOV eliminano la latenza introdotta dall'elaborazione basata su software della connessione.

Perché è stata scelta la modalità di backup attivo per le porte SR-IOV sulla VM CPNR

La modalità di collegamento Active-Backup è particolarmente adatta per questa implementazione, grazie alla semplicità, alla tolleranza di errore e alla compatibilità con le interfacce SR-IOV. Ecco perché:

1. Ridondanza senza complessità

- Modalità Active-Backup: Solo un'interfaccia (l'interfaccia attiva) trasmette e riceve traffico alla volta. Le altre interfacce rimangono in modalità standby.
- Se l'interfaccia attiva non funziona (ad esempio a causa di un errore di collegamento o di un problema hardware), il collegamento passa automaticamente a un'interfaccia di standby. Ciò garantisce una connettività di rete continua senza richiedere interventi manuali.

2. Non è richiesto alcun LAG (Link Aggregation Group)

- A differenza di altre modalità di collegamento (ad esempio,802.3adorbalance-alb), la modalità Active-Backup non richiede configurazioni LACP (Link Aggregation Control Protocol) o switch-side.
- Ciò è particolarmente importante per le porte SR-IOV, in quanto le VF SR-IOV in genere non supportano le configurazioni LACP o LAG.

3. Failover continuo

- Failover quasi istantaneo con interruzione minima del traffico.
- Quando l'interfaccia attiva non funziona, il collegamento promuove immediatamente un'interfaccia di standby allo stato attivo.

4. Indipendenza dall'hardware

La modalità Active-Backup funziona indipendentemente dagli switch fisici o dall'hardware sottostanti. La logica di failover risiede interamente nel kernel Linux, rendendolo estremamente versatile e portatile.

5. Ottimizzato per SR-IOV

Le VF SR-IOV sono legate a NIC e nodi NUMA fisici specifici. Utilizzando la modalità Active-Backup, è possibile combinare VF di nodi NUMA diversi in un'unica interfaccia di collegamento logico (bond0). Ciò garantisce un'elevata disponibilità e un uso efficiente delle risorse NUMA.

La modalità Active-Backup è una delle modalità più semplici e più utilizzate nel collegamento Linux. È stato progettato per fornire elevata disponibilità garantendo che il traffico continui a

scorrere senza problemi anche in caso di errore di una delle interfacce collegate. Si tratta di una spiegazione dettagliata del funzionamento della modalità Active-Backup, delle caratteristiche principali e dei vantaggi.

Che cos'è un'interfaccia Linux Bond?

Un'interfaccia di collegamento in Linux combina due o più interfacce di rete in un'unica interfaccia logica. Questa interfaccia logica, nota come legame (ad esempio, bond0), viene utilizzata per fornire:

- Ridondanza: Garanzia di elevata disponibilità della connettività di rete.
- Miglioramento delle prestazioni: In altre modalità (ad esempio,balance-error802.3ad), può anche aggregare la larghezza di banda.

Funzionamento Della Modalità Backup Attivo

Nella modalità Active-Backup, per trasmettere e ricevere il traffico viene usata una sola interfaccia (chiamata interfaccia attiva) alla volta. Le altre interfacce rimangono in modalità standby. Se l'interfaccia attiva non funziona, una delle interfacce in standby viene promossa allo stato attivo e il traffico viene automaticamente reindirizzato alla nuova interfaccia attiva.

Caratteristiche principali della modalità Active-Backup

1. Interfaccia attiva singola:

    - In qualsiasi momento, solo un'interfaccia fisica nel bond è attiva per la trasmissione e la ricezione del traffico.
    - Le interfacce in standby sono completamente passive a meno che non si verifichi un failover.

2. Failover automatico:

    - Se l'interfaccia attiva non funziona (ad esempio a causa di un problema hardware, di una disconnessione del cavo o di un errore di collegamento), il collegamento passa automaticamente a un'interfaccia di standby.
    - Il failover è senza interruzioni e non richiede interventi manuali.

3. Supporto failback:

    Una volta ripristinata, l'interfaccia guasta può riattivarsi automaticamente (se è stata configurata per farlo) o rimanere in modalità standby, a seconda della configurazione di legame.

4. Nessun requisito per il lato switch:

- A differenza di altre modalità di collegamento (ad esempio,802.3adorbalance-rr), la modalità Active-Backup non richiede alcuna configurazione speciale sugli switch fisici (ad esempio, LAG o LACP).
- Questo lo rende ideale per scenari in cui la configurazione lato switch non è possibile o quando si collegano le funzioni virtuali SR-IOV, che non supportano il LAG.

5. Monitoraggio

    - Il collegamento controlla continuamente lo stato di tutte le interfacce membro utilizzando il parametro `imon`(Media Independent Interface Monitor).
    - Se viene rilevato un errore di collegamento, il collegamento passa immediatamente a un'interfaccia di standby integra.

Modalità di flusso del traffico in modalità backup attivo

Funzionamento normale

1. Interfaccia attiva:

    - Il traffico scorre esclusivamente attraverso l'interfaccia attiva (ad esempio,eth2in un legame eth2e deth3).
    - L'interfaccia di standby (eth3) rimane inattiva e non trasmette o riceve traffico.

2. Monitoraggio

    - Il bond controlla periodicamente lo stato di tutte le interfacce membro. A tale scopo, utilizzare:
        - miimon Controlla lo stato del collegamento di ciascuna interfaccia a un intervallo configurabile (ad esempio, ogni 100 ms).
        - Monitoraggio Address Resolution Protocol (ARP) (facoltativo): Invia richieste ARP per verificare che l'interfaccia attiva sia raggiungibile.

Scenario di failover

1. Errore di collegamento su interfaccia attiva:

    Se l'interfaccia attiva (eth2) non funziona (ad esempio, il cavo non è collegato, si è verificato un errore hardware della scheda NIC o il collegamento non funziona), il collegamento rileva immediatamente il problema utilizzando il monitoraggio miimonon o ARP.

2. Failover automatico:

    - Il collegamento passa all'interfaccia di standby (eth3), che diventa la nuova interfaccia attiva.
    - Il traffico viene reindirizzato tramite la nuova interfaccia attiva senza richiedere un intervento manuale.

3. Tempestività del failover:

   Il processo di failover è quasi istantaneo (in genere entro pochi millisecondi, a seconda di temiimoninterval).

Scenario di failback

1. Ripristino dell'interfaccia non riuscita:

   - Quando l'interfaccia precedentemente guasta (eth2) viene ripristinata, può:
     - Recuperare automaticamente il ruolo attivo (se configurato per tale operazione).
     - Rimanere in modalità standby (comportamento predefinito).

2. Continuità del traffico:

   Il failback è senza interruzioni e garantisce l'assenza di interruzioni per i flussi di traffico in corso.

Scenario d'uso: Collegamento Active-Backup con porte SR-IOV

La modalità Active-Backup è particolarmente indicata per le interfacce SR-IOV in quanto:

- Le VF SR-IOV in genere non supportano protocolli di aggregazione dei collegamenti come LACP.
- Il collegamento in modalità Active-Backup può fornire ridondanza senza alcuna configurazione sul lato switch.

Ad esempio:

- eth2 è mappato a una VF SR-IOV onsriov0(nodo NUMA 0).
- eth3 è mappato a una VF SR-IOV onsriov1(nodo NUMA 1).
- Il collegamento (bond0) combina queste interfacce, fornendo un failover senza problemi tra VF SR-IOV.

Passaggio 1. OpenStack Networking

Il CPNR VNF richiede le quattro reti seguenti:

1. Rete di orchestrazione: Per il traffico di controllo e orchestrazione (basato su Openvswitch).
2. Rete di gestione: Per accesso amministrativo (basato su Openvswitch).
3. Rete SR-IOV 1: Traffico applicazione/servizio su sriov0.
4. Rete SR-IOV 2: Traffico applicazione/servizio su sriov1.

Installazione dettagliata:

Passaggio 1.1. Creazione Di Reti Openvswitch

- Rete di orchestrazione:

```
openstack network create --provider-network-type vxlan orchestration-network
```

- Rete di gestione:

```
openstack network create --provider-network-type vxlan management-network
```

Passaggio 1.2. Creazione di subnet per le reti Openvswitch

- Subnet orchestrazione:

```
openstack subnet create --network orchestration-network \
--subnet-range 192.168.100.0/24 orchestration-subnet
```

- Subnet di gestione:

```
openstack subnet create --network management-network \
--subnet-range 10.10.10.0/24 management-subnet
```

Passaggio 1.3. Creazione di reti SR-IOV

- Rete SR-IOV 1:

```
openstack network create --provider-network-type vlan \
--provider-physical-network sriov0 --provider-segment 101 sriov-network-1
```

- Rete SR-IOV 2:

```
openstack network create --provider-network-type vlan \
--provider-physical-network sriov1 --provider-segment 102 sriov-network-2
```

Passaggio 2. OpenStack Flavors

Passaggio 2.1. Creazione di un gusto per i numeri incrociati

Per garantire che il VNF sia in grado di accedere alle schede di interfaccia di rete SR-IOV da entrambi i nodi NUMA, creare una configurazione con supporto cross-NUMA:

```
openstack flavor create --ram 8192 --vcpus 4 --disk 40 cross-numa-flavor
```

Passaggio 2.2. Configurazione delle proprietà NUMA

Impostare le proprietà specifiche di NUMA:

```
openstack flavor set cross-numa-flavor \
--property hw:numa_nodes=2 \
--property hw:cpu_policy=dedicated \
--property hw:mem_page_size=large
```

Passaggio 3. Configurare il collegamento in modalità Active-Backup

Dopo aver avviato il VNF, configurare l'interfaccia di collegamento per le porte SR-IOV (eth2 e eth3) sul VNF.

Passaggio 3.1. Configurazione dell'interfaccia del bond

Creare un'interfaccia di collegamento (bond0) in modalità Active-Backup:

```
vi /etc/sysconfig/network-scripts/ifcfg-bond0
```

```
DEVICE=bond0
BOOTPROTO=static
ONBOOT=yes
BONDING_OPTS="mode=active-backup miimon=100"
IPADDR=172.16.1.10
NETMASK=255.255.255.0
GATEWAY=172.16.1.1
```

Passaggio 3.2. Configurazione delle interfacce slave

- eth2:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth2
```

```
DEVICE=eth2
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

- eth3:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth3
```

```
DEVICE=eth3
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Passaggio 3.3. Applicazione della configurazione

Riavviare il servizio di rete per applicare la configurazione:

```
systemctl restart network
```

Verifica

Dopo aver distribuito il file VNF, verificarne la funzionalità attenendosi alla seguente procedura:

1. Verifica dello stato VNF

Verificare che l'istanza VNF sia attiva:

```
openstack server show cpnr-instance
```

Assicurarsi che lo stato sia ACTIVE.

2. Verifica della connettività di rete

- Test Ping: Verificare che il VNF sia in grado di comunicare su tutte le reti:

  ```
  ping
  ```

  ```
  ping
  ```

- Interfaccia bond:
  - Confermare che bond0 sia attivo:

    ```
    cat /proc/net/bonding/bond0
    ```

    Cerca:
    - Slave attualmente attivo: Indica l'interfaccia attiva.
    - Interfaccia slave: Conferma che sia l'opzione 2 che l'opzione 3 fanno parte del vincolo.

3. Verifica posizionamento NUMA

Verificare che il VNF utilizzi le risorse di entrambi i nodi NUMA:

```
nova show

        --human | grep numa
```

Procedure ottimali

- Monitoraggio e risoluzione dei problemi: Utilizzare strumenti quali cpdumpandethtoolper monitorare le interfacce SR-IOV.
- Security: Gestire con attenzione l'accesso alla rete fisica e applicare un rigoroso isolamento tra i tenant.
- Proporzioni: Pianificare la capacità della scheda NIC fisica durante la scalabilità delle installazioni SR-IOV, in quanto il numero di VF disponibili è limitato dall'hardware della scheda NIC.

Risoluzione dei problemi

Se la distribuzione non funziona come previsto, fare riferimento alla procedura di risoluzione dei problemi seguente:

1. Verificare la configurazione di SR-IOV

- Verificare se SR-IOV è abilitato nel BIOS:

```
dmesg | grep -i "SR-IOV"
```

- Verificare che le VF siano state create sulle schede NIC:

```
lspci | grep Ethernet
```

2. Verifica posizionamento NUMA

Se il VNF non è in grado di accedere a entrambe le schede NIC, verificare che sia abilitata la modalità cross-NUMA:

- Controllare le proprietà NUMA del gusto:

```
openstack flavor show cross-numa-flavor
```

3. Emissioni dell'interfaccia per le obbligazioni

- Verificare lo stato dell'obbligazione:

```
cat /proc/net/bonding/bond0
```

- Se l'obbligazione non funziona:
  - Verificare che le interfacce slave (eth2eeth3) siano configurate correttamente come parte del collegamento.
  - Riavviare il servizio di rete:

```
systemctl restart network
```

4. Problemi di connettività di rete

- Verificare i binding della porta OpenStack:

```
openstack port list --server cpnr-instance
```

- Verificare la corretta configurazione IP nel VNF:

```
ip addr show
```

Conclusioni

La distribuzione di VNF CPNR su OpenStack con porte SR-IOV richiede la modalità cross-NUMA per consentire al VNF di connettersi alle schede NIC da entrambi i nodi NUMA. Questo è essenziale perché OpenStack limita le VNF in modalità Single-NUMA ad accedere solo alle risorse (NIC, CPU, memoria) all'interno del nodo NUMA in cui viene avviato il VNF. La combinazione della modalità inter-NUMA con il collegamento Active-Backup garantisce elevata disponibilità, tolleranza di errore e utilizzo efficiente delle risorse, rendendo questa implementazione estremamente resiliente e performante.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).